Amendments to the Claims

This listing of claims supersedes all listing of claims.

In the Claims

Please amend the claims as follows:

1. (Currently amended) In a wireless data communications system wherein mobile units communicate with a computer using access points, and wherein said system operates according to a protocol specifying a format for data message packets and said data message packets contain state information for said mobile units, a method for detecting unauthorized access attempts to the system, comprising:

forwarding one or more data packets received by said access points to a computer, said state table on said computer, said state table storing state information for said mobile units, the state information including at least a MAC address parameter, an authentication status parameter, and a further parameter unrelated to the MAC address parameter and the authentication status parameter and maintaining a state transition history for each of said mobile units; and

operating said computer to compare format and state information of said one or more received data packets to selected requirements of said protocol-specified format and said stored state information, and signaling an alert if said packets deviate from said protocol-specified format or said stored state information.

2. (Original) A method as specified in claim 1 wherein said protocol-specified format includes a header message and wherein said comparing of format comprises comparing format of said header message portion to said protocol-specified format.

3. (Canceled)

4. (Previously presented) A method as specified in claim 2 wherein said protocol is a wireless protocol having a frame control field in said header message portion and wherein said comparing of format comprises comparing format of said frame control field.

5. (Previously presented) A method as specified in claim 1 wherein said one or more received data packets comprise Management Frames.

6. (Previously presented) A method as specified in claim 1 wherein said one or more received data packets comprise Control Frames.

7. (Previously presented) A method as specified in claim 1 wherein said one or more received data packets comprise a first WEP flag.

8. (Previously presented) A method as specified in claim 7 wherein said packets have a first WEP flag value which is inconsistent with a second WEP value stored in said state table on said computer.

9. (Previously presented) A method as specified in claim 1 wherein said one or more received data packets comprise a first Protocol Version value which is inconsistent with a second Protocol Version value stored in said state table on said computer.

10. (Original) A method as specified in claim 1 wherein said one or more received data packets comprise a source MAC address which is a multicast address.

11. Original) A method as specified in claim 1 wherein said one or more received data packets comprise a source MAC address which is a broadcast address.

12. (Previously presented) A method as specified in claim 1 wherein said one or more received data packets comprise a first Power Management state variable which is inconsistent with a second Power Management state variable value stored in said state table on said computer.

13. (Previously presented) A method as specified in claim 1 wherein the step of

operating said computer further comprises checking a More Data field of said received data packets for a value of "1" and further monitoring said access points for a possible denial of service attack.

14. (Previously presented) A method as specified in claim 1 wherein said one or more received data packets comprise an unsupported Type value.

15. (Previously presented) A method as specified in claim 1 wherein said one or more received data packets comprise an unsupported Type value.

16. (Original) A method as specified in claim 1 wherein said one or more received data packets comprise a spoofed MAC address.

17. (Previously presented) A method as specified in claim 1 wherein said one or more received data packets comprise a frame of length which is inconsistent with said protocol-specified format.

18. (Canceled)

19. (Currently amended) In a wireless data communications system wherein mobile units communicate with a computer using access points, and wherein said system operates according to a protocol specifying a format for data message packets and said data message packets contain state information for said access points, a method for detecting unauthorized access attempts to the system, comprising:

forwarding one or more data packets received by said mobile units to a computer; 4

maintaining a state table on said computer, said state table storing state information for said access points, the state information including at least a MAC address parameter, an authentication status parameter, and a further parameter unrelated to the MAC address parameter and the authentication status parameter and maintaining a state transition history for each of said mobile units; and

operating said computer to compare format and state information of said one or more received data packets to selected requirements of said protocol-specified format and said stored state information, and signaling an alert if said packets deviate from said protocol-specified format or said stored state information.

20. (Original) A method as specified in claim 19 wherein said protocol-specified format includes a header message portion and wherein said comparing of format comprises comparing format of said header message portion to said protocol-specified format.

21. (Previously presented) A method specified in claim 20 wherein said protocol is a wireless protocol having a frame control field in said header message portion and wherein said comparing of format comprises comparing format of said frame control field.

22. (Previously presented) A method as specified in claim 19 wherein said one or more received data packets comprise Management Frames.

23. (Previously presented) A method as specified in claim 19 wherein said one or more received data packets comprise Control Frames.

24. (Canceled)

25. (Previously presented) A method as specified in claim 19 wherein said one or more received data packets comprise a first WEP flag.

26. (Previously presented) A method as specified in claim 25 wherein said packets have a first WEP flag value which is inconsistent with a second WEP value stored in said state table on said computer.

27. (Previously presented) A method as specified in claim 25 wherein said one or more received data packets comprise a first Protocol Version value which is inconsistent with a second Protocol Version value stored in said state table on said computer.

28. (Previously presented) A method as specified in claim 19 wherein said one or more received data packets comprise a source MAC address which is a multicast address.

29. (Previously presented) A method as specified in claim 19 wherein said one or more received data packets comprise a source MAC address which is a broadcast address.

30. (Previously presented) A method as specified in claim 19 wherein said one or more received data packets comprise a first Power Management state variable which is inconsistent with a second Power Management state variable value stored in said state table on said computer.

31. (Previously presented) A method as specified in claim 19 wherein the step of operating said computer further comprises checking a More Data field of said received data packets for a value of "1 " and further monitoring said access points for a possible denial of service attack.

32. (Previously presented) A method as specified in claim 19 wherein said one or more received data packets comprise an unsupported Type value.

33. (Previously presented) A method as specified in claim 19 wherein said one or more received data packets comprise an unsupported SubType value.

34. (Previously presented) A method as specified in claim 19 wherein said one or more received data packets comprise a spoofed MAC address.

35. (Previously presented) A method as specified in claim 19 wherein said one or more received data packets comprise a frame of length which is inconsistent with said protocol-specified format.

36. (Canceled)

37. (Canceled)

38. (Canceled)

39. (Canceled)

40. (New) The method of Claim 1, wherein said further parameter is a power management mode.

41. (New) The method of Claim 19, wherein said further parameter is a power management mode.